Networking Requirements

Welcome to Clinton Connect! We're happy you've chosen our solution for both loss prevention and digital signage. To make the process of platform adoption easier, we've put together this technical onboarding guide. Here you'll find information on how the Connect platform is designed to work, networking requirements that can be shared with IT, as well as installation information. Hopefully this document answers all of your questions. However, if you find anything missing you may always contact support to get a fast and friendly answer.

IT Quickstart

Connect PVMs are designed to be internet-connected devices managed through a web-based user interface. Here are some technical details to help you fast track connectivity.

IP Addresses

- All Connect PVMs require one IP address to support remote management of content.
- PVMs equipped with IP cameras will require an additional IP address.
- Connect PVMs were designed with DHCP in mind. Static IP addresses may be achieved by using MAC address reservation at your router. Assigning a static IP address at the device is not currently supported. (This pertains to the adapter used for content management only; static IPs may be assigned to the IP camera through the camera management software.)

Required Whitelisting

In order to function fully, the web application and Connect PVMs need to be able to connect to the following URLs:

- https://api.clintonconnect.com
- https://media.clintonconnect.com
- wss://ws-mt1.pusher.com:433

We often receive requests for IP address when IT departments set up whitelisting on their networks. As Clinton Connect is a cloud-based platform, the IP addresses of the above services may change over time. For this reason we ask that whitelisting be done by URL rather than IP address.

Network Speed Requirements

Connect PVMs require a minimum connection speed of 2 Mbps down (comparable to a 3G wireless connection). Using a slower network connection will result in exceedingly long content download times. We recommend a connection of 20 Mbps (comparable to a 4G wireless connection) or faster.

Connect Platform Overview

The Clinton Connect platform is a secure, cloud-based network designed to allow users to manage deployment of advertising materials to thousands of devices from anywhere in the world. The cloud-based architecture alleviates the hassles of installation, setup and network management as there is no port-forwarding or static IP address required. This also makes the platform more secure. No open or forwarded ports means less exposure to potential attackers. All connections between Clinton Connect devices are encrypted, and communication is restricted to our servers only

This following is an overview of the Clinton Connect security strategy across the entire platform. Currently, the platform consists of three components: the Connect Cloud Services, Web Client, and the Connect Public View Monitor (PVM). While developing the Clinton Connect platform, we have taken steps to ensure the security of each of these components individually and as a whole. That commitment to the security of your data continues as the platform grows. Below is a brief introduction to each of the platform components.

Connect Cloud Services

The Connect Cloud Services are the backbone of the Clinton Connect platform. Both the Web Client and the PVM Client communicate with the Connect Cloud Services to be able to process the information they need to do each of their individual jobs. The Connect Cloud Services handles network requests, communications with third-party services, business logic, and data storage.

As you can tell, the Connect Cloud Services play a central part in network architecture. All network communications flow in and out of our cloud services. The Connect Cloud Services consist of three parts: Virtual Private Cloud, Cloud Storage/CDN, and Real-time Messaging. The Virtual Private Cloud handles all incoming communications from both the web client and PVM. It handles incoming files and places them in Cloud Storage. The CDN handles serving files both to the web client and PVM. Lastly, Realtime Messaging responsible for direct communication from Connect Cloud Services out to Connect Web Clients and PVMs. As these are mission-critical to our platform, all Connect Cloud Services employ multiple redundancies, and all communications in, out, and between services are encrypted.

Connect Platform Overview Continued...

Web Client

The Web Client is the portal that Clinton Connect users use to access and manipulate their data. The web client is accessible via a web browser at https://app.clintonconnect.com. Through a password-protected portal users may manage devices, upload media, and create and deploy ads to their devices. The web client connects via an encrypted connection directly to the Connect Cloud Services in order to do so. This involves communicating with our Virtual Private Cloud servers, downloading content from our Content Delivery Network (CDN), and receiving realtime messages from our Realtime Messaging service. All functionality of the Clinton Connect platform is initiated through the Web Client. For example, Company Users may log in to upload media, create advertisements, and deploy schedules. Company Owners may log in to manage access to their company's data. Integrators may log in to create a new Company and prepare for PVM installations across that Company's stores.

Connect PVM

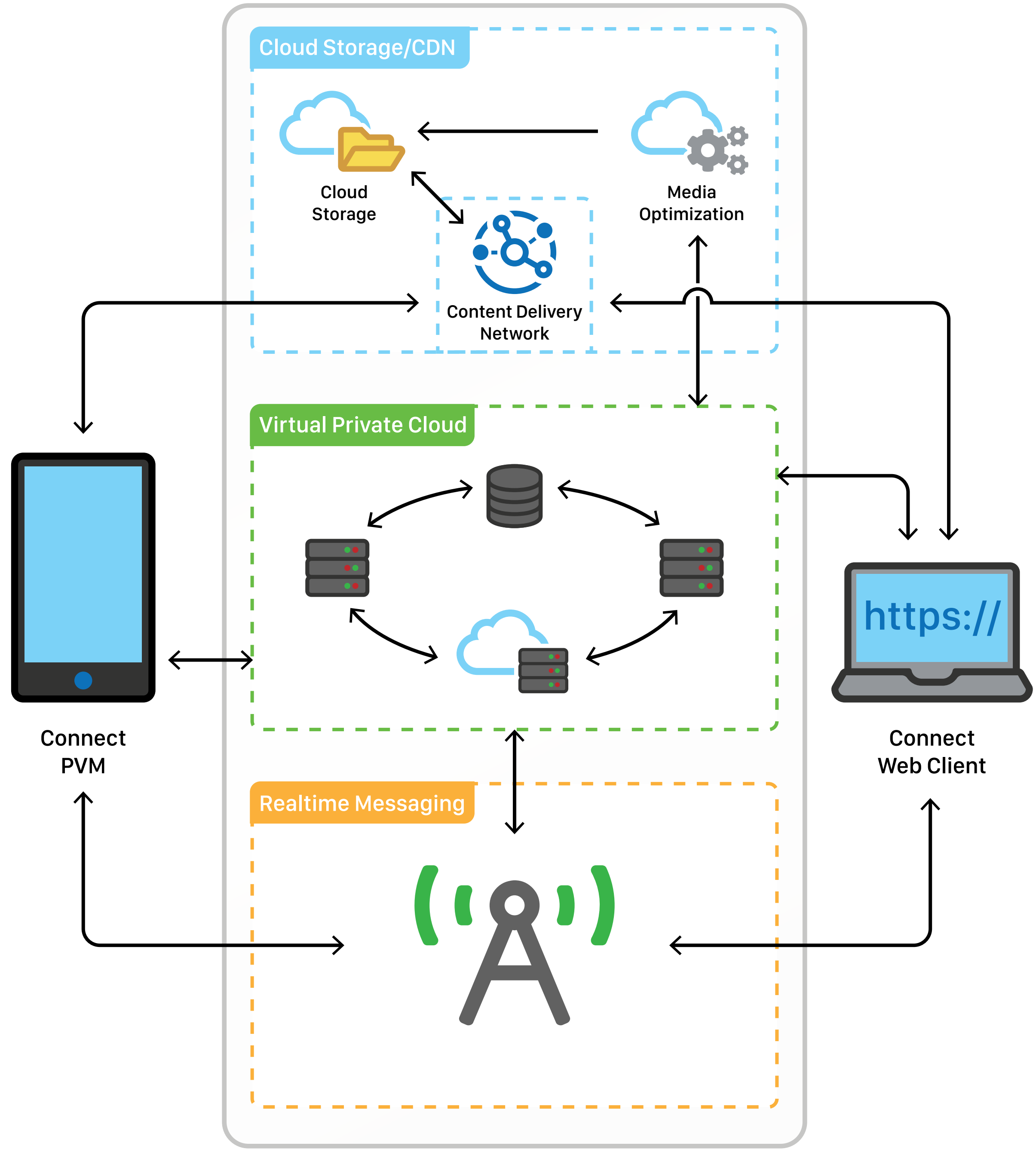
The Connect PVM consists of both the hardware PVM itself as well as the software which runs it. The Connect PVM is in many ways like a traditional PVM. It uses a camera to display a live video feed on its screen, providing a theft deterrent. However— the Connect PVM also employs an on-board computer that can download media and display advertising on the screen, making it part of the Clinton Connect platform.

The Connect PVM is the most visible piece of the platform, as there may be thousands of connected devices receiving content to display on their screen for customers to see. Devices establish an internet connection during an onboarding process where it will be connected to a network either by ethernet or wifi. As long as the device can reach the internet (and specifically our servers), that is all the network setup required.

When a user deploys content to a device via the Connect Web Client, our Connect Cloud Services send a notification to the PVM to alert it that new content is available. At that time the PVM connects securely to the CDN to download the needed content and display it on the screen.

Apart from deploying content, users may also manipulate certain aspects of the PVM remotely via the web client. For example, LED settings and volume may be controlled remotely, and the device may be rebooted remotely. Similarly to the deployment process, these changes are pushed from our Connect Cloud Services out to the devices.

Network Diagram



Security Strategy

The security strategy of the Clinton Connect platform is a multi-layered strategy that includes both software and hardware considerations. Precautions take into account both accidental and malicious incidents. Below we will describe specific steps we have taken regarding potential vulnerabilities and how they apply to each of the platform components.

Network Communications

All data on the Clinton Connect platform is encrypted while in transit. This means that all data sent between the Server and Web Client, Connect PVM and Server, and between the Server and any third-party services remains encrypted via industry-standard SSL technology (HTTPS). The Web Client and Connect PVM only require a connection to our Server, push notification service, and our file server. Network admins may easily limit traffic on their network to these three sources - making their network even more secure. In the case of high network load, or a network-based attack such as a Distributed Denial of Service (DDoS), we employ a load balancer and request rate limits to keep the application running. We can ban traffic from offending IP addresses if needed.

Identity Protection

All access to the Clinton Connect platform (specifically, access to the Server via the Web Client) requires a login by username and password. It is a closed ecosystem in that users may not self-enroll. A user may only be issued account access by a privileged user. We employ a tiered Access Control List based on Roles and Permissions to prevent people from accessing and manipulating sensitive data. For example, users must have sufficient permissions to deploy a schedule to potentially thousands of devices. Other permissions are required for setting up new companies and users.

Two-Factor Authentication (2FA) has become a standard way for users to add an extra layer of Identity Protection. 2FA increases security by requiring not only something a user knows (their password) but also something they possess (typically their phone) to gain access to their account. Once a user enters their correct password, they must also provide a code which is either sent to or generated by their phone. 2FA is only available by request and will require a third party "authenticator service," such as Google Authenticator or Authy.

While the Connect PVMs are not technically users, they do connect to the Clinton Connect platform and therefore must be authenticated. Each Connect PVM receives an access token during installation, and all access to the Server via the Connect PVM is protected by authentication via an access token.

Data Storage

Data stored in the Clinton Connect platform is protected against loss. Database backups are made nightly and stored for an extended period. Most data is never deleted immediately, only marked for deletion at a later date. This way, we can easily restore items "accidentally" deleted by any user. The Web Client and the Connect PVM are both designed as "thin clients," meaning they store very little data locally, and any data can easily be restored to them from the Server.

All files stored in Clinton Connect (such as images and videos used for advertisements) are stored on servers designed for mission-critical primary data storage. It is a highly-redundant environment capable of sustaining the concurrent loss of two data centers and offering a 99.99% availability.

Physical/Hardware Security

While many security precautions are software-related, potential vulnerabilities have been addressed on a physical/hardware level as well. Clinton Connect uses hardware owned by various third-party services for computing power, data storage, and file storage. These services are chosen in part because of their commitment to the security of their clients. We use only world-class, enterprise-level service providers who are among the top ten such service providers in the world.

Among their touted physical security features are the following:

- A globally-redundant infrastructure
- 24/7 physical security guard services
- CCTV coverage externally and internally for the facility
- Biometric readers with two-factor authentication
- Battery and generator backup

The Connect PVM itself has been designed with security in mind. All Connect PVMs are constructed with a ruggedized steel case with an acrylic vandal-resistant face. Access to all physical access ports (USB, Ethernet, etc.) is protected behind a steel panel held in place with a vandal-resistant Torx screw.

Summary

Clinton Electronics takes the security of your data very seriously. We have designed the Clinton Connect platform from the ground up with security in mind. Be it software or hardware solutions, preventing accidental loss or malicious attacks, we are committed to providing a platform you can trust. This commitment continues as we continually improve the security of the platform.

Need Help? Give us a call: 800-549-6393

Our technical support staff is here to help you with any difficulty you may have and regularly goes above and beyond to ensure your satisfaction every time.